GROUP USER REVOCATION AND PUBLIC INTEGRITY AUDITING FOR SHARED DYNAMIC CLOUD DATA

K.BOOPATHI
Assistant Professor
Department of Computer Science
GTN Arts College, Dindigul, Tamilnadu, India

Abstract : Cloud computing is an important storage platform being researched nowadays. The enhancement of cloud computing make storage outsourcing becomes an exceeding trend, which result a secure data auditing a cool topic that emerge in research literature. Recently some researches consider the problem of efficient and secure public data authentication inspection for shared dynamic data. However, these schemes are still not secure against the collusion and leakage of cloud storage server from unauthorized attacker and revoked group users during user revocation in cloud storage system. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user cancelation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the scheme definition. Our scheme keeping the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Finally, the security and experimental analysis show that compared with its relevant schemes our scheme is also secure and efficient.

IndexTerms - Cloud computing, TPA, Public Auditing

I. INTRODUCTION

The improvements and enhancements in cloud computing motivates organization as well as enterprises to outsource their data to third party cloud service providers (CSP's) which will result in improvements the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) [1] on-line data backup services of Amazon and software like Google Drive, [2] Dropbox, [3] Mozy, [4] Bitcasa and [5] Memopal built for cloud application. In some cases cloud server sometime returns invalid results such as hardware/software failure, malicious attack and human maintenance. Security and privacy of cloud user's data should be protected by data integrity and accessibility. To overcome the security issues of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme are not sufficient for practical application. For achieving the integrity and availability of remote cloud storage, some various solutions and their different variants have been proposed. In these solutions, when a scheme supports modification of data, it is known as dynamic scheme, otherwise static one. A scheme is *publicly verifiable* that means the integrity check of data can be performed not only by data owners, but also by the third party auditor (TPA). However, the focus of the dynamic scheme is on the cases where only and only data owner could modify the data of cloud. Recently, the development of cloud computing emerged some applications where the services of cloud can be used as a collaboration platform. In these software development environments, one or more than one (multiple) users in a group need to share source code as well as they needs to access, compile, modify and run the source code share by user at any time. The new model of cooperation network in cloud provides the infeasibility of data for auditing the remote data, where only the data owner can update its data. It will result in terrific communication and computation to the data owner which causes the single point of data owner. To achieve multiple data operation, Wang et al. put forth data integrity based on ring signature. In the scheme, it does not consider the user revocation problem and the cost of auditing is linear to the data size and group size. To further raise up the previous scheme and support group user revocation, Wang et al. proposed a scheme based on proxy re-signatures. However, this scheme assumes that authenticated and private channels exist between the pair of entities and there is no collusion among them. Also, cost of auditing the scheme is linear to the size of the group. Another attempt to improve the previous scheme and make the scheme scalable, efficient and collusion resistant, Yuan and Yu designed a dynamic public integrity auditing scheme with group user revocation. However, in their scheme, the authors do not consider the secrecy of data among the group users. That means, their scheme could efficiently support plain text of data update and integrity auditing, while not ciphertext data. In their scheme, if data owner shares group key among the users of group, revocation of any group user allow the group users to update their shared key. Also, the owner of the data does not take part in the user revocation phase, where the user revocation phase is itself conducted by the cloud. In this case, the malicious cloud server will result in collusion of revoked user and the cloud server where the cloud server could update data number of times as designed and provide a legal data finally.

Due to above mentioned deficiency; we propose a construction which includes data encryption and decryption during the data modification processing, secure and efficient user revocation and also removal of redundant data. Here, vector commitment scheme will be applied over the database. Then we apply the Asymmetric Group Key Agreement (AGKA) and group signatures to support ciphertext database update among group users and efficient group user revocation respectively. The user in the group will be able to encrypt or decrypt a message from any other group users when the group users use the AGKA

protocol to encrypt or decrypt the share database. The collusion of the cloud and revoked group users will be prevented by the group signature.

II RELATED WORK

J. Yuan and S. Yu,[6] presented efficient public integrity checking for cloud data sharing with multi-user modification in which is featured by salient properties of public integrity checking and continual computational cost on user side. We achieve this through our novel design on polynomial based authentication tags which allows accumulation of tags of different data blocks. X. Chen, J. Li, J. Weng, J. Ma, and W. Lou,[7] proposed verifiable computation over large database with incremental updates. Authors formalize the notion of verifiable database with incremental updates (Inc-VDB). Besides, they propose a general Inc-VDB framework by incorporating the primitive of vector commitment and the encrypt-thenincremental MAC mode of encryption. They present a concrete Inc-VDB scheme based on the computational Diffie- Hellman (CDH) assumption and prove that system can achieve the desired security properties.

E. Shi, E. Stefanov, and C. Papamanthou,[8] proposed practical dynamic proofs of retrievability with constant client storage whose bandwidth cost is comparable to a Merkle hash tree, thus being very practical. There construction outperforms the constructions of Stefanov et al. and Cash et al., both in theory and in practice. Specifically, for n outsourced blocks of β bits each, writing a block requires β +O(λ log n) bandwidth and O(β log n) server computation (λ is the security parameter). Audits are also very efficient, requiring β + O(λ 2 log n) bandwidth. They also show how to make there scheme publicly verifiable, providing the first dynamic PoR scheme with such a property. They finally provide a very efficient implementation of our scheme. B. Wang, L. Baochun, and L. Hui,[9] presented public auditing for shared data with efficient user revocation in the cloud. By utilizing the idea of proxy re-signatures, they allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud.

C. Wang, Q. Wang, K. Ren, and W. Lou,[10] presented privacy-preserving public auditing for data storage security in cloud computing utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files.

Boyang Wang, Baochun Li and Hui Li are the members of IEEE explore the concept of "Oruta: Privacy-Preserving Public Auditing for Shared data in the Cloud" in 2014. It shows that services of cloud provide not only data storage in commonplace, but also data sharing across multiple users. However, it remains an open challenge to audit the shared data by preserving identity privacy. This system proposed public auditing of shared data stored in cloud by using privacy preserving mechanism. In particular, this paper exploits the concept of group signature which computes the verification information required for integrity auditing of shared data. With this mechanism, the signer identity of each block in shared data remains private from a third party auditor (TPA) which can publicly verify shared data integrity without accessing entire data. In extend this mechanism support batch auditing. This mechanism is responsible for auditing multiple shared data in just single auditing task. The high level comparison between Oruta and its relevant existing systems are shown in following Table 1. This paper represent first attempt towards designing effective public auditing of shared data in the cloud storage by preserving privacy.

	PDP [2]	WWRL [3]	ORUTA
Public Auditing	Yes	Yes	Yes
Data Privacy	No	Yes	Yes
Identity Privacy	No	No	Yes

Table 1 Comparison with Existing Mechanism

As illustrated in Fig., the work in this paper involves three parties: the cloud server, the third party auditor (TPA) and users. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices.

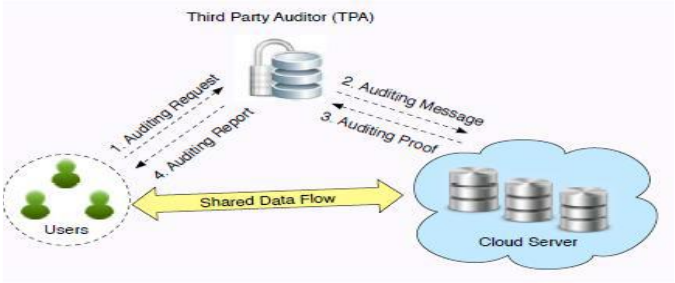

Fig.1 System Architecture

III PROBLEM FORMULATION

System architecture

Proposed scheme consists of three entities: Group users, Cloud storage server and Third Party Auditor (TPA), as shown in the Fig. 2.

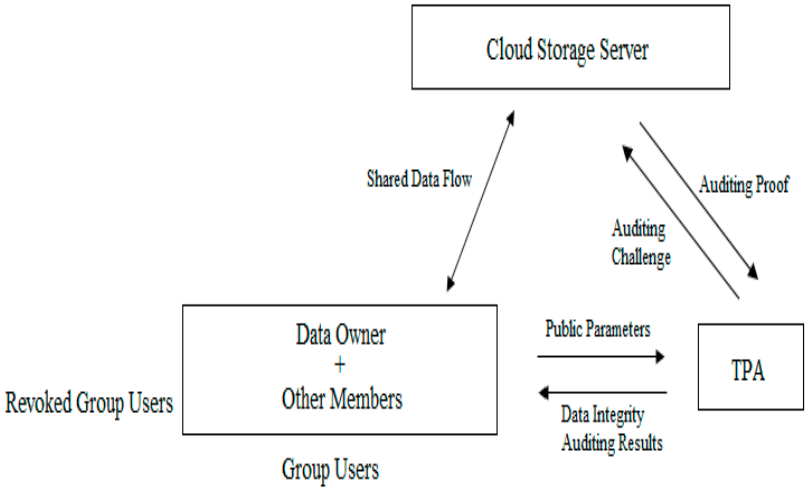

Fig. 2: System architecture

• Group users: They consist of data owners & other members of the group with whom the data owner can share his stored data along with privileges to access, modify etc. it.

• Cloud storage server: It is responsible for providing storage services to the cloud user. It is semi-trusted and hence, attacks are possible.

• Third Party Auditor: It is liable for verifying the integrity of stored data upon request. It audits the file and sends back the result.

System design

• Data owner: If a cloud user wants to share some data amongst a number of users then he will be acting as a data owner. Data owner may share his stored data among the members of an existing group or can create a new group which will include only those members with whom he wants to share the data. If he do not want to share some of his data with any member, he can easily do so. Moreover, he has the privilege to secure his data by encrypting it before uploading on the cloud. Fig. 3 showcases the jobs a data owner can do.

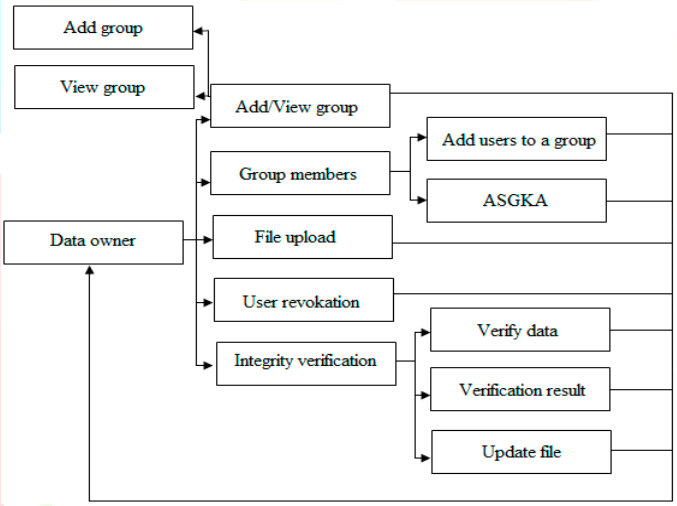

Fig 3 Data Owner

• **Cloud server:** Cloud server is the remote storage server for the users data. All the data uploaded by the data owner is stored at this storage server. Since it is semi trusted, it is possible that the cloud may try to gain access to the stored data as shown in the Fig. 4. Such an attempt by the cloud server is unacceptable and this type of unauthorized access to stored data with the purpose to view or modify it, leaves data owners data vulnerable. Thus to protect the revelation of data if such an attempt is made by the cloud server, data should be encrypted before being stored at a remote location which adds a level of security to the stored data.

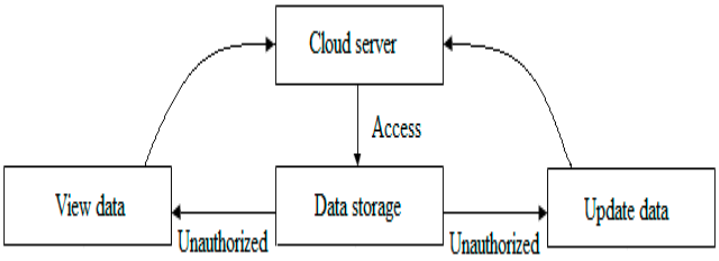

Fig.4 Cloud Server

• **Third Party Auditor:** It is liable for verifying data integrity when requested by a member of the group as shown in Fig. 5. Whenever a request to verify integrity comes, it generates a challenge & sends it to cloud server. TPA upon getting a response from the cloud performs the auditing task & sends the result back to the user.

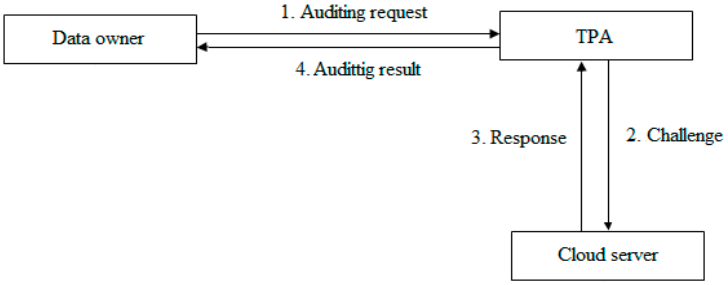

Fig.5 Third Party Auditor

IV EXISTING SYSTEM

For providing the integrity and availability of faraway cloud store, existing systems provides some solutions. In these solutions, when a scheme helps data modification, we call it dynamic scheme, otherwise static one (or limited dynamic scheme, if a scheme could only efficiently support some specified operation, such as append). A scheme is openly verifiable means that the data integrity check can be performed not only by data owners, but also by any third-party auditor. However, the dynamic schemes above focus on the cases where there is a data owner and only the data owner could modify the data. The user revocation problem is not examine and the auditing cost is linear to the group size and data size.

Disadvantage:

1) The user revocation problem is not considered and the auditing cost is linear to the group size and data size.
2) In previous systems could efficiently support plaintext data update and integrity auditing, while not cipher text data.
3) In their scheme, if the data owner trivially shares a group key among the group users, the defection or revocation any group user will force the group users to update their shared key.
4) The data owner does not take part in the user revocation phase, where the cloud itself could conduct the user revocation phase.
5) The collusion of revoked user and the cloud server will give chance to malicious cloud server where the cloud server could update the data as many time as designed and provide a legal data finally.

V PROPOSED SYSTEM APPROACH

We propose a new idea called Public Integrity Auditing for shared dynamic cloud data with group user revocation which explore how to design an efficient and reliable scheme, while accomplishing secure group user revocation. The system not only keeps group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation. The proposed system, inspect on the secure and efficient shared data integrate auditing for multi-user operation for cipher text database. It proposes an efficient data auditing scheme while at the same time providing some new features, such as traceability and countability.

Advantage:

1) Provides data integrate auditing for multi-user operation for cipher text database.
2) Provide the security and efficiency analysis of our scheme.
3) Provide reliability, confidentiality, traceability and countability.

A. DATA OWNER:

Data owner is responsible for uploading file on cloud as well as view files uploaded by him or others. Data owner must have to register in our system.

B. DATA USER:

Data user is the one who is responsible for downloading files or view files uploaded by data owners. To download file from cloud he has to be authenticated user otherwise he will be considered as attacker.

C. THIRD PARTY AUDITOR(TPA):

Third party auditor is an authorized person who has rights to validate authorized data owner and user. He is also responsible for allocation of block and maintains information and authentication.

D. CLOUD STORAGE SERVER:

Cloud storage server holds files or data of the data owner on the cloud. Data owner must have to pay charges for this.

VI CONCLUSION

The first of verifiable database with efficient updates is an eventful way to solve the problem of verifiable outsourcing of storage. We propose a scheme to clear up efficient and secure data integrity auditing for share dynamic data with multiuser modification. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the amalgamating of the three primitive enable our scheme to outsource cipher text database to remote cloud and support secure group users revocation to shared dynamic data. We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. Also, the performance analysis shows that, compared with its pertinent schemes, our scheme is also efficient in different phases.

REFERENCES

[1] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015

[2] Hugo E. Camacho, J. Alfredo Brambila, Alfredo Peña, José M. Vargas, "A cloud environment for backup and data storage," in Engineering Information Technology, Polytechnic University of Altamira, Altamira Tamaulipas, México

[3] Jin Li, Yan Kit Li, X. Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorize Deduplication," in Proc. of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM VOL:PP NO:99 YEAR 2014

[4] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, " Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" in Proc. Of IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 201X

[5] C. Wang Student Member, IEEE, Sherman S.-M. Chow, Q. Wang, Student Member, IEEE, K. Ren, Member, IEEE, and W. Lou, Member, IEEE , "Privacy-Preserving Public Auditing for Secure Cloud Storage".

[6] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014,Toronto, Canada, Apr. 2014, pp. 2121–2129.

[7] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," in Proc. of ESORICS 2014, Wroclaw, Poland, Sep. 2014, pp. 148–162.

[8] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 325–336.

[9] B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preservingpublic auditing for data storage security in cloud computing,"inProc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp. 525–533